

## TITLE OF THE INVENTION

SECURITY MONITOR APPARATUS AND METHOD USING SMART CARD

## CROSS-REFERENCE TO RELATED APPLICATION

**[0001]** This application claims the benefit of Korean Patent Application No. 2002-58463, filed on September 26, 2002, in the Korean Intellectual Property Office, the disclosure of which is incorporated herein by reference.

## BACKGROUND OF THE INVENTION

### 1. Field of the Invention

**[0002]** The present invention relates to computer security, and more particularly, to a security monitor apparatus and method using a smart card that contains personal information.

### 2. Description of the Related Art

**[0003]** As environmental protection and energy savings are matters of major concern, screen protection and energy conservation are becoming increasingly important considerations in a system that includes a monitor. For instance, a screen saver or Display Power Management Signaling (DPMS) is commonly used in a display apparatus, such as a monitor, in order to reduce power consumption.

**[0004]** A power-saving screen saver for a computer monitor changes the current monitor mode to screen protection mode when user input e.g., through a mouse or keyboard is lacking for a predetermined time. While in a screen protection mode, computer activation requires user input or a predetermined password.

**[0005]** DPMS is an international standard focused on achieving a reduction in monitor power consumption. The standard defines four types of power modes corresponding to Advanced Power Management (APM) employed by the main body of a computer. APM is an API developed by INTEL and MICROSOFT allowing power management to be written into the system BIOS. The APM's four types of power modes are an on-mode, a stand-by mode, a suspend mode, and an off-mode. In the on-mode, vertical and horizontal synchronization signals are input from a computer to a display apparatus via a connector. During the on-mode, a video signal is input to the computer and displayed on a screen, operating at full power. In the stand-by mode, only a vertical synchronization signal is input from the computer to the display apparatus via the connector. Nothing is displayed on the screen due

to the blanking of the video signal. The screen operates at partial power usage, resulting in little power consumption. In the suspend mode, only a horizontal synchronization signal is input from the computer to the display apparatus via the connector. Once again, nothing is displayed on the screen due to the blanking of the video signal. The screen operates at minimal power usage, resulting in little power consumption. In the off-mode, the power supply is completely shut off, and the vertical and horizontal synchronization signals are not input to the display apparatus. The video signal is blanked, resulting in maximum power savings.

**[0006]** However, the aforementioned screen saver, DPMS-type monitor protection, and energy saving modes unfortunately are not operational until a lack of user input has been detected after a predetermined time. Therefore, actions for monitor protection cannot be immediately taken. Also, once screen saver mode has been set, the existing screen saver mode requires the input of a predetermined password, creating an inconvenience to the user.

#### SUMMARY OF THE INVENTION

**[0007]** The present invention provides a security monitor apparatus that allows immediate screen protection and power savings using a smart card with personal identification information, and a method using the same.

**[0008]** According to an aspect of the present invention, a system is provided comprising a smart card that contains personal identification information, and a display unit that reads the personal identification information from the smart card and determines whether the display of the display unit will be turned on or off based on the reading result.

**[0009]** According to another aspect of the present invention, a monitor is connected to a system and displays a signal generated by the system. The monitor includes an interface that is used to communicate with the smart card containing personal identification information, a detector that detects a signal through the interface to determine insertion of the smart card into the monitor, and a controller that reads the personal identification information via the interface from the smart card, and controls turning the display of the monitor on or off when the insertion of the smart card is detected.

**[0010]** According to another aspect of the present invention, the controller registers personal identification information stored in the smart card and deletes the registered personal identification information. The monitor may further include a storage unit that stores the personal identification information from the smart card during the registration

function. The personal identification information may be deleted from the storage unit. Also, the controller may turn the display of the monitor off when the detector does not recognize the presence of the smart card.

**[0011]** According to yet another aspect of the present invention, a method is provided of turning a display of a monitor on or off that is connected to a system, generating a signal for the monitor to display, using a smart card containing personal identification information . The method includes checking the insertion of the smart card into the monitor, turning the display of the monitor off when the smart card is not inserted into the monitor, reading the personal identification information from the smart card when the smart card is inserted into the monitor, turning the display of the monitor on when the personal identification information relates to an authenticated user, and turning the display of the monitor off when the personal identification information does not relate to the authenticated user.

**[0012]** According to another aspect of the present invention, whether the personal identification information relates to the authenticated user is determined by checking whether information stored in a storage unit of the monitor is the same as the personal identification information stored in the smart card.

**[0013]** According to another aspect of the present invention, the method includes a registration process in which the personal identification information is read from the smart card and stored in the storage unit for the authentication of personal identification information. The method further includes a deletion process in which the information registered to the storage unit is deleted.

**[0014]** According to still another aspect of the present invention, a method is provided of turning a display of a monitor that is connected to a system on or off, and generating a signal for the monitor to display, using a smart card. The method includes registering information stored in the smart card to a storage unit of the monitor, checking the insertion of the smart card into the monitor through a smart card interface on the monitor, and turning the display of the monitor on when the insertion of the smart card is detected and information stored in the smart card is the same as that stored in the storage unit. The method further includes deleting the information from the storage unit of the monitor.

**[0015]** According to still another aspect of the present invention, a monitor is provided that is connected to a system and displays a signal generated by the system . The monitor includes an interface that allows a signal to be input to, and output from, a smart card containing personal identification information, a detector that detects a signal output through

the interface, to determine if the smart card is inserted, into or removed, from the monitor . A controller implements an on-screen display (OSD) region on a screen of the monitor and displays into the OSD region registration and deletion buttons of the personal identification information and an authentication result from checking the personal identification information, and turns the display of the monitor on or off based on the authentication result, when the detector determines the insertion of the smart card.

**[0016]** According to another aspect of the present invention, the method includes storing the personal identification information that is read from the smart card during a registration function of the controller. Also, the personal identification information may be deleted from the storage unit during a deleting operation by the controller. The controller turns the display of the monitor off when the detector transmits to the controller a signal indicating that the smart card is removed from the monitor.

**[0017]** Additional aspects and advantages of the invention will be set forth in part in the description which follows and, in part, will be obvious from the description, or may be learned by practice of the invention.

#### BRIEF DESCRIPTION OF THE DRAWINGS

**[0018]** These features, and/or other aspects and advantages of the invention will become apparent and more readily appreciated from the following description of the embodiments taken in conjunction with accompanying drawings in which:

**[0019]** FIG. 1 is a block diagram of a security monitor apparatus using a smart card according to an aspect of the present invention;

**[0020]** FIG. 2 is a flowchart illustrating a security monitor method using a smart card according to an aspect of the invention;

**[0021]** FIG. 3A is a flowchart illustrating the registering operation illustrated in FIGS. 1 and 2;

**[0022]** FIG. 3B is a flowchart illustrating the deleting operation illustrated in FIGS. 1 and 2; and

**[0023]** FIG. 3C is a flowchart illustrating a management method that disables the security monitor method according to an aspect of the invention.

## DETAILED DESCRIPTION OF THE INVENTION

**[0024]** Reference will now be made in detail to the embodiments of the present invention, examples of which are illustrated in the accompanying drawings wherein like reference numerals refer to the like elements throughout. The embodiments are described below in order to explain the present invention by referring to the figures.

**[0025]** The present invention provides a monitor apparatus, which recognizes a smart card containing personal identification information and controls activation of the monitor apparatus based on the recognition result.

**[0026]** FIG. 1 is a block diagram of a security monitor apparatus using a smart card according to an aspect of the present invention. For example, a computer monitor is selected as a monitor apparatus .

**[0027]** The monitor of FIG. 1 is connected to a system (not shown) such as a computer and displays a signal generated by the system. The monitor includes an interface 100 allowing information to be input to, and output from, a smart card (not shown) containing personal identification information, and a detector 110 determining insertion of the smart card into the monitor . A controller 120 reads the personal identification information from the smart card via the interface 100 and controls a turning on or off of the display of the monitor based on the read result, when the presence of the smart card is recognized by the detector 110.

**[0028]** The interface 100, which is a smart card holder, includes a smart card connector. An input signal, an output signal, a clock signal, and a reset signal are input to, and output from, the smart card through connection terminals SM\_I/O, SM\_CLK, and SM\_RST of the smart card connector.

**[0029]** The detector 110 circuit outputs different electrical signals, depending on whether the smart card is inserted into or removed from the monitor .

**[0030]** The controller 120 includes a smart card controller 121 and a monitor microcomputer 122. The smart card controller 121 provides a clock signal to the smart card via the connection terminal SM\_CLK, i.e. a clock terminal, of the smart card connector on the interface 100, and resets an input/output operation of a signal to/from the smart card using the connection terminal SM\_RST, i.e. a reset terminal. Also, the smart card controller 121 reads information, such as the personal identification information, from the smart card via the connection terminal SM\_I/O, i.e. an input/output signal terminal, and returns an

acknowledge signal ACK to the smart card, acknowledging receipt of a command or a signal.

**[0031]** The monitor microcomputer 122, controlling monitor display, receives an electrical signal from the detector 110, indicating the insertion or removal of the smart card into the monitor. If the electrical signal indicates the insertion of the smart card, the microcomputer 122 has a power supplier 140 provide power to the smart card so that the smart card is charged with electricity, and resulting in the flow of signals in the smart card. When the personal identification information stored in the smart card is output, using the smart card controller 121, to the microcomputer 122, the microcomputer 122 checks whether the information relates to an authenticated user, and controls the display of the monitor based on the checking result. In other words, the microcomputer 122 activates the monitor display when the personal identification information is authenticated, and deactivates the monitor display of the monitor otherwise.

**[0032]** The smart card controller 121 or the microcomputer 122 performs an initial registration process in which the personal identification information is stored in a storage device (or memory) 130 of the smart card using an external input device, such as a keyboard or a mouse, and an on-screen display (OSD) function of the monitor. For instance, when the personal identification information is first read from the smart card and displayed on the monitor, in an OSD state, "confirm" or "cancel" buttons are also displayed so that the user can register or delete the information using one of the "confirm" and "cancel" buttons. If the user selects a registration icon, using the mouse or the keyboard, the personal identification information read from the smart card controller 121 is stored in the storage unit 130. The stored personal identification information is used in determining whether or not information to be read from a smart card in the future is related to an authenticated user. Similarly, a "delete" button can be provided in the OSD allowing a user to delete personal identification information which has already been registered and stored in the storage unit 130.

**[0033]** The controller 120 turns the display of the monitor off when it does not receive a signal from the detector 110 indicating insertion of the smart card. The controller 120 also turns the monitor off, when information read from a smart card through the interface 100 does not match information stored in the storage unit 130.

**[0034]** FIG. 2 is a flowchart illustrating a security monitor method using a smart card, and a controller included in a monitor apparatus. Referring to FIG. 2, the insertion of a smart card into the cardholder installed in a monitor apparatus is checked e.g., by a controller, as

shown in operation 200. If the presence of the smart card is not detected after a predetermined time, the controller shuts off the supply of power to the monitor turning the display of the monitor off, in operation 210. If the presence of the smart card is detected, the controller reads personal identification information from the smart card in operation 220. Power is supplied to the smart card, in a security monitor apparatus as shown in FIG. 1, prior to reading the personal identification information from the smart card.

**[0035]** Next in operation 230, the personal identification information read from the smart card is examined for relation to an authenticated user. In other words, the information read from the smart card is compared with information of an authenticated user. The information of an authenticated user may originate from a smart card read for the first time, and stored in the storage unit 130 as explained with respect to the apparatus of FIG. 1. If the information currently being read from the smart card correlates to the information of the authenticated user, the display of the monitor is turned on, if off, in operation 240. Otherwise, the display of the monitor is turned off in operation 250. At this time, a warning may first be displayed on the monitor using an OSD, indicating that information read from the smart card is not related to an authenticated user.

**[0036]** FIGS. 3A through 3C are flowcharts illustrating methods of managing a smart card according to aspects of the present invention.

**[0037]** More specifically, FIG. 3A is a flowchart illustrating the registration process described with reference to FIGS. 1 and 2.

**[0038]** Referring to FIG. 3A, the insertion of a smart card into a monitor is checked in operation 301. If the presence of the smart card is detected, personal identification information is read from the smart card in operation 302. The method of FIG. 3A may further include supplying power to the smart card prior to reading the information therefrom, when the presence of the smart card is detected. After reading the information from the smart card, the information is stored e.g., in a storage unit of the monitor in operation 303. The registration process may be automatically performed in the monitor or performed through a user interface by an interaction with a user when information stored in the smart card is read for the first time.

**[0039]** FIG. 3B is a flowchart illustrating the deletion of personal identification information stored in a storage unit, described with reference to the FIGS. 1 and 2. Referring to FIG. 3B, the insertion of a smart card into a monitor is checked in operation 311. If the presence of the smart card is detected, personal identification information is read from the smart card in

operation 312. The method of FIG. 3B may also include supplying power to the smart card prior to reading the information therefrom, when the presence of the smart card is detected. After operation 312, it is checked whether the read information is the same as that stored in a storage unit of the monitor in operation 313. If the information of the two are the same, the information stored in the storage unit is deleted in operation 314. Here, the deletion is performed by a user through interaction with a user interface.

**[0040]** FIG. 3C is a flowchart illustrating a management method disabling the monitor security method according to another aspect of the present invention. Referring to FIG. 3C, an OSD, instructing a user to input a predetermined password to be recognized by a monitor, is displayed on the monitor in operation 321. Then, when the user inputs a password, the user input is authenticated in operation 322. If the user input is authenticated, use of the smart card to control the display of the monitor is disabled in operation 323.

**[0041]** As described above, a smart card containing personal identification information is inserted into a monitor apparatus facilitating immediate screen protection and power saving.

**[0042]** According to other aspects of the invention, the smart card controller 121 or the microcomputer 122 is a computer implementing the methods in FIGS. 2, 3A, 3B, and 3C using data encoded on a computer-readable medium.

**[0043]** Although a few embodiments of the present invention have been particularly shown and described, it would be appreciated by those skilled in the art that changes may be made therein in these embodiments without departing from the principles and spirit of the invention, the scope of which is defined in the claims and their equivalents.